What is claimed is:

1. A method of increasing peer privacy, comprising:

receiving a request for data from a data requestor, wherein said data is stored at a data provider;

selecting a plurality of peers to form a path, wherein said data provider and said data requestor are the respective ends of said path;

generating a mix according to said path; and

transmitting said mix to said data provider.

2. The method according to claim 1, further comprising:

generating a first encryption key; and

encrypting said first encryption key with a public encryption key of said data provider.

3. The method according to claim 2, further comprising:

encrypting said reference to said data with said first encryption key; and

encrypting said first encryption key with a public encryption key of said data requestor.

4. The method according to claim 4, further comprising:

transmitting said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key

with said public encryption key of said data requestor to said data provider as a message to said data provider.

5. The method according to claim 4, further comprising:

receiving said message at said data provider;

decrypting said first encryption key with a complementary encryption key to said public key of said data provider; and

decrypting said data reference with said first encryption key.

6. The method according to claim 5, further comprising:

modifying said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieving said data according to said data reference;

encrypting said data with said first encryption key; and

transmitting said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

7. The method according to claim 5, further comprising:

receiving said modified message at a current peer along said path;

modifying said mix with a complementary encryption key of said current peer to obtain a next peer along said path; and

transmitting said modified mix along with said encrypted data and said first encryption key of said data requestor as another modified message to said next peer.

8. The method according to claim 1, wherein said generation of said mix further comprises:

generating a decoy mix.

9. The method according to claim 8, further comprising:

forming a tuple comprising said data requestor and said decoy mix; and

modifying said mix by encrypting said tuple with an encryption key of a peer subsequent to said data requestor in said path.

10. The method according to claim 9, wherein said encryption key comprises an public encryption key.

11. The method according to claim 10, wherein said public encryption key is generated by one of an asymmetric encryption algorithm.

12. The method according to claim 1, wherein said generation of said mix further comprises:

selecting a current peer along said path;

forming a current tuple comprising said current peer and a previous mix; and

modifying said mix at said current peer by encrypting said current tuple with an encryption key of a subsequent peer to said current peer in said path.

13. The method according to claim 12, further comprising:

repeating said formation and modification until said current peer being said data provider.

14. A method of increasing peer privacy, comprising:

receiving a message comprising a mix at a current peer;

modifying said mix by applying a complementary encryption key of said current to said mix;

retrieving a subsequent peer to said current peer;

modifying said message with said modified mix; and

transmitting said modified message to said subsequent peer.

15. The method according to claim 14, further comprising:

selecting a plurality of peers to form a path; and

generating said mix according to said path.

16. The method according to claim 14, further comprising:

adding encrypted requested data to said message from a data provider.

17. The method according to claim 14, further comprising:

generating a decoy mix, wherein said mix includes said decoy mix.

18. A system for increasing privacy, comprising:

at least one processor;

memory coupled to said at least one processor; and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to:

receive a request for a data from a data requestor, wherein said data is stored at a data provider;

select a plurality of peers to form a path, wherein said data provider and said data requestor are the respective ends of said path;

generate a mix according to said path; and

transmit said mix to said data provider.

19. The system according to claim 18, wherein said privacy module is also configured to generate a first encryption key and to encrypt said first encryption key with a public encryption key of said data provider.

20. The system according to claim 19, wherein said privacy module is further configured to encrypt said reference to said data with said first encryption key and to encrypt said first encryption key with a public encryption key of said data requestor.

21. The system according to claim 20, wherein said privacy module is further configured to transmit said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key with

said public encryption key of said data requestor to said data provider as a message to said data provider.

22. An apparatus for increasing privacy in a data requestor, comprising:

at least one processor;

memory coupled to said at least one processor; and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider, said message comprises:

a mix configured to provide a path among a plurality of peers;

an encrypted reference to requested data encrypted with a first encryption key;

an encrypted first encryption key protected with a public key of said data requestor; and

said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider and to decrypt said data reference with said first encryption key.

23. The system according to claim 22, wherein said privacy module is further configured to:

modify said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieve said data according to said data reference.

encrypt said data with said first encryption key; and

transmit said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

24. A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of increasing peer privacy, said one or more computer programs comprising a set of instructions for:

receiving a request for a data from a data requestor, wherein said data is stored at a data provider;

selecting a plurality of peers to form a path, wherein said data provider and said data requestor are the respective ends of said path;

generating a mix according to said path; and

transmitting said mix to said data provider.

25. The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

generating a first encryption key; and

encrypting said first encryption key with a public encryption key of said data provider.

26. The computer readable storage medium in according to claim 25, said one or more computer programs further comprising a set of instructions for:

encrypting said reference to said data with said first encryption key; and

encrypting said first encryption key with a public encryption key of said data requestor.

27. The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

transmitting said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key with said public encryption key of said data requestor to said data provider as a message to said data provider.

28. The computer readable storage medium in according to claim 27, said one or more computer programs further comprising a set of instructions for:

receiving said message at said data provider;

decrypting said first encryption key with a complementary encryption key to said public key of said data provider; and

decrypting said data reference with said first encryption key.

29. The computer readable storage medium in according to claim 28, said one or more computer programs further comprising a set of instructions for:

modifying said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieving said data according to said data reference;

encrypting said data with said first encryption key; and

transmitting said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

30. The computer readable storage medium in according to claim 29, said one or more computer programs further comprising a set of instructions for:

receiving said modified message at a current peer along said path;

modifying said mix with a complementary encryption key of said current peer to obtain a next peer along said path; and

transmitting said modified mix along with said encrypted data and said first encryption key of said data requestor as another modified message to said next peer.

31. The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

generating a decoy mix.

32. The computer readable storage medium in according to claim 31, said one or more computer programs further comprising a set of instructions for:

forming a tuple comprising said data requestor and said decoy mix; and

modifying said mix by encrypting said tuple with an encryption key of a peer subsequent to said data requestor in said path.

33. The computer readable storage medium in according to claim 32, said one or more computer programs further, wherein said encryption key comprises an public encryption key.

34. The computer readable storage medium in according to claim 33, said one or more computer programs further, wherein said public encryption key is generated by one of a symmetric encryption algorithm and an asymmetric encryption algorithm.

35. The computer readable storage medium in according to claim 24, said one or more computer programs further, , wherein said generation of said mix further comprises:

selecting a current peer along said path;

forming a current tuple comprising said current peer and a previous mix; and

modifying said mix at said current peer by encrypting said current tuple with an encryption key of a subsequent peer to said current peer in said path.

36. The computer readable storage medium in according to claim 35, said one or more computer programs further comprising a set of instructions for:

repeating said formation and modification until said current peer being said data provider.